CLAIMS

1-6. (canceled)

7. (original) A method for verifying the legitimacy of an untrusted signature verification mechanism, comprising:

submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and said second signature being known to be unverifiable;

receiving a response from the untrusted mechanism for each submission of either said first signature or said second signature;

determining whether each response received from the untrusted mechanism is a correct response; and

in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate.

8. (original) The method of claim 7, wherein said sequence is generated randomly.

9. (original) The method of claim 8, wherein said sequence is generated using a random number generator.

10. (original) The method of claim 7, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature.

11. (original) The method of claim 7, wherein determining whether each response received from the untrusted mechanism is a correct response comprises:

where the signature submitted to the untrusted mechanism was said first signature, determining whether the response from the untrusted mechanism is that said first signature is verified; and

where the signature submitted to the untrusted mechanism was said second signature, determining whether the response from the untrusted mechanism is that said second signature is not verified.

12-17. (canceled)

18. (original) An apparatus for verifying the legitimacy of an untrusted signature verification mechanism, comprising:

a mechanism for submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and said second signature being known to be unverifiable;

a mechanism for receiving a response from the untrusted mechanism for each submission of either said first signature or said second signature;

a mechanism for determining whether each response received from the untrusted mechanism is a correct response; and

a mechanism for determining, in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, the untrusted mechanism to not be legitimate.

19. (original) The apparatus of claim 18, wherein said sequence is generated randomly.

20. (original) The apparatus of claim 19, wherein the mechanism for submitting comprises a random number generator.

21. (original) The apparatus of claim 18, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature.

22. (original) The apparatus of claim 18, wherein the mechanism for determining whether each response received from the untrusted mechanism is a correct response comprises:

a mechanism for determining, where the signature submitted to the untrusted mechanism was said first signature, whether the response from the untrusted mechanism is that said first signature is verified; and

a mechanism for determining, where the signature submitted to the untrusted mechanism was said second signature, whether the response from the untrusted mechanism is that said second signature is not verified.

23-28. (canceled)

29. (original) A computer readable medium having stored thereon instructions which, when executed by one or more processors, cause the one or more processors to verify the legitimacy of an untrusted signature verification mechanism, said computer readable medium comprising:

instructions for causing one or more processors to submit a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and said second signature being known to be unverifiable;

instructions for causing one or more processors to receive a response from the untrusted mechanism for each submission of either said first signature or said second signature;

instructions for causing one or more processors to determine whether each response received from the untrusted mechanism is a correct response; and

instructions for causing one or more processors to determine, in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, the untrusted mechanism to not be legitimate.

30. (original) The computer readable medium of claim 29, wherein said sequence is generated randomly.

31. (original) The computer readable medium of claim 30, wherein said sequence is generated using a random number generator.

32. (original) The computer readable medium of claim 29, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature.

33. (original) The computer readable medium of claim 29, wherein the instructions for causing one or more processors to determine whether each response received from the untrusted mechanism is a correct response comprises:

instructions for causing one or more processors to determine, where the signature submitted to the untrusted mechanism was said first signature, whether the response from the untrusted mechanism is that said first signature is verified; and

instructions for causing one or more processors to determine, where the signature submitted to the untrusted mechanism was said second signature, whether the response from the untrusted mechanism is that said second signature is not verified.

34. (canceled)